Topics:
non-state IT [2], privacy [3], state business [4], BYOD [5], mobility [6]

Non-State Technology and Computing Devices [1]

SS-12-002 Non-State Technology and Computing Devices

Issue Date: 4/04/2012

Revision Effective Date: 4/04/2012

PURPOSE:

The State of Georgia owns or has custodial responsibility for the information accessed, created, transmitted or stored on behalf of the State or in conducting official State business and has ultimate responsibility for protecting that information regardless of the medium used. The proliferation of non-State technology devices used to conduct business on behalf of the State has made it essential that the State establish standards that contemplate their existence and use.

This standard expands upon the rules governing information security to specifically include use of non-State technology devices. It intends to communicate the State?s intent and commitment to safeguard sensitive information for which it has responsibility and to discourage the rampant and careless use of non-State technology devices.

STANDARD

Use of non-State technology devices to perform agency functions is at the discretion of the agency. Agencies shall establish and document internal polices and standards governing the use of non-State technology devices to access non-public State information assets. Such use shall comply with all applicable laws, regulations, policies and standards governing information and data security including but not limited to appropriate use, access, boundary and media controls, records management, retention and e-discovery.

Agencies allowing the use of non-State technology devices shall conduct risk assessments in accordance with State standards, and shall explicitly include the use of non-State technology devices in the appropriate system security plans. When conducting its risk assessment the agency shall consider such items as:

- The State worker already has access to the sensitive information in the course of their duties.
- Possible controls to minimize the impact of lost or stolen devices such as encryption, remote wiping or locking capabilities or GPS tracking.
- Additional compensating controls deployed to minimize new risks.
- Federal requirements that some types of information require the device to be destroyed or wiped to a particular federal standard when the employee no longer has access to the information.
- Laws pertaining to the use of non-State technology devices in the workplace are relatively new and untested in court. The agency should consult with legal counsel regarding their standard and ability to enforce it.

EXCEPTIONS:

This standard does not apply to:

- All access to the public domain.
- State employees accessing State networks, using non-State devices, for the sole purpose of conducting personal business such as accessing individual personnel, benefits, medical and/or other private human